Method for the secure handling of monetary or value units using prepaid data carriers

Patent number:	DE19860203
Publication date:	2000-06-29
Inventor:	WANKO CLEMENS (DE); KORST UWE K H (DE)
Applicant:	DEUTSCHE TELEKOM AG (DE)
Classification:	
- international:	G06F17/60; G07F7/08; G07F19/00
- european:	G07F7/08C2B; G07F7/10D2; G07F7/10D2K; G07F7/10D4E2
Application number:	DE19981060203 19981224
Priority number(s):	DE19981060203 19981224

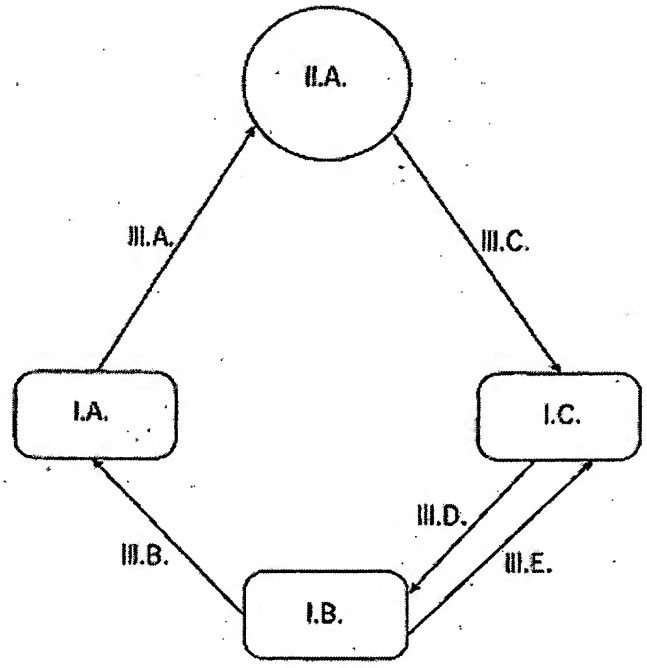
Also published as:

WO0039758 (A1)
EP1141904 (A1)
US6745940 (B1)

Report a data error here

Abstract of **DE19860203**

The invention relates to a payment method in public telecommunications systems by means of pre-paid chip cards, especially in the form of memory chip cards or microprocessor chip cards. The card value is managed in a central background system and the communication is entirely controlled by said background system. According to the invention, a chip, for example a telephone card, is personalised, i.e. provided with a definite identification number of identification characteristic, by the card provider (I A). A value is assigned to the identification characteristic. Said value, however, is not saved on the chip of the data carrier. The value is made available, together with the identification characteristic, for a background system (I B) via a communications channel (III B). The identification characteristic and the value are saved in a data bank in the communications channel. The identification characteristic is provided with the label "not cleared". Said label is cancelled by the data bank just before the respective card is actually sold which makes the value ready for debiting in the background system. A customer (2) can use such a chip card (II A) in a communications terminal (I C) which is designed therefor, whereby only the identification characteristic is read out from the card in order to forward said identification characteristic to the background system (I B) and request a debit (III D). The background system (I B) can release the original value that has been assigned in the personalisation process, allocate said value to the identification characteristic and confirm the debit (III E). The communications link is directly created and controlled by the background system. A link can thus be cut after debiting of the entire card value in the data bank of the background system (I B) using said background system (I B).



(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 60 203 A 1**

(51) Int. Cl.[7]:
G 06 F 17/60
G 07 F 7/08
G 07 F 19/00

(21) Aktenzeichen: 198 60 203.0
(22) Anmeldetag: 24. 12. 1998
(43) Offenlegungstag: 29. 6. 2000

(71) Anmelder:
Deutsche Telekom AG, 53113 Bonn, DE

(72) Erfinder:
Wanko, Clemens, 63322 Rödermark, DE; Korst, Uwe K. H., 64625 Bensheim, DE

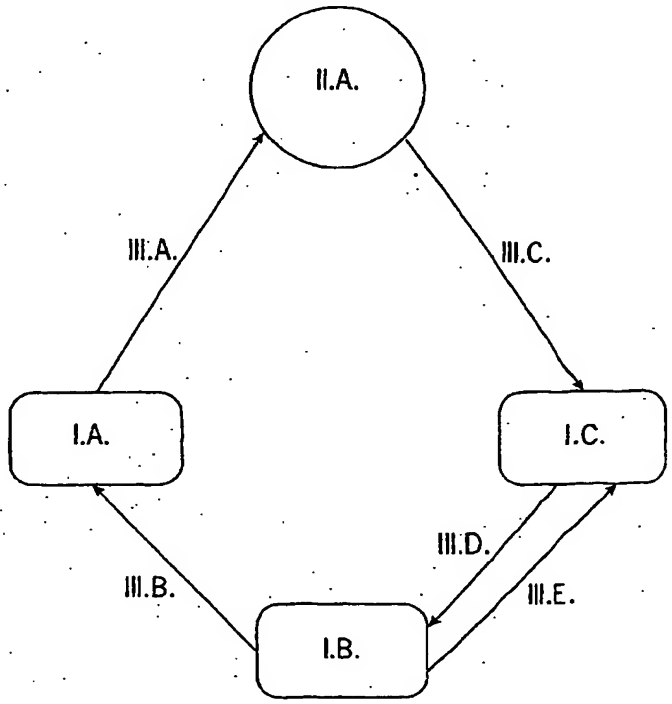
(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE 197 14 259 A1
DE 195 39 801 A1
DE 44 26 486 A1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

(54) Verfahren für die sichere Handhabung von Geld- oder Werteeinheiten mit vorausbezahlten Datenträgern

(57) Es wird ein Verfahren für die Bezahlung in der öffentlichen Telekommunikation mittels vorausbezahlter Chipkarten, insbesondere in Form von Speicherchipkarten oder Mikroprozessorchipkarten, beschrieben, wobei der Kartenwert in einem zentralen Hintergrundsystem verwaltet wird und die Kommunikation vollständig durch das Hintergrundsystem gesteuert wird. Dabei wird ein Chip, zum Beispiel einer Telefonkarte, durch den Kartenausgeber (IA) personalisiert, das heißt mit einer eindeutigen Identifikationsnummer bzw. einem Identifikationsmerkmal versehen. Dem Identifikationsmerkmal wird ein Wert zugeordnet, der jedoch nicht auf dem Chip des Datenträgers gespeichert wird. Der Wert wird zusammen mit dem Identifikationsmerkmal einem Hintergrundsystem (IB) über einen Kommunikationsweg (IIIB) verfügbar gemacht. Dort wird das Identifikationsmerkmal zusammen mit dem Wert in einer Datenbank gespeichert und zunächst mit dem Vermerk "nicht freigeschaltet" versehen. Unmittelbar vor dem eigentlichen Verkauf der jeweiligen Karte wird dieser Vermerk in der Datenbank entfernt und damit steht der Wert im Hintergrundsystem zur Abbuchung bereit. Ein Kunde (2) kann eine derartige Chipkarte (IIA) an einem hierfür vorgesehenen öffentlichen Kommunikationsterminal (IC) nutzen, wobei lediglich das Identifikationsmerkmal aus der Karte ausgelesen wird, um es an das Hintergrundsystem (IB) weiterzuleiten und eine Buchungsanfrage (IIID) durchzuführen. Das Hintergrundsystem (IB) kann nun dem ...



DE 198 60 203 A 1

DE 198 60 203 A 1

BNSDOCID: <DE_____19860203A1_I_>

Beschreibung

Die Erfindung betrifft ein Verfahren für die sichere Handhabung von Geld- oder Werteeinheiten mit vorausbezahlten Datenträgern nach dem Oberbegriff des Patentanspruchs 1.

Konzepte für das Betreiben von elektronischen Geldbörsen auf Chipkarten befinden sich bereits seit einigen Jahren sowohl in der Entwicklung als auch im Einsatz. Sie beinhalten neben der Technik der Chipkarte in den meisten Fällen auch die Sicherheitstechnik für das Zusammenwirken von Chipkarte und Rechner- und Übertragungssystemen sowie die Abrechnung der mit der Chipkarte vorgenommenen Transaktionen. Sowohl national als auch international wurden bereits zahlreiche Konzepte vorgestellt. In einigen Ländern sind elektronische Geldbörsensysteme eingesetzt, wie zum Beispiel

- Feldversuch Eisenstadt, Österreich, seit Dezember 1994
- Avantcard – in Finnland
- Danmond Konzept in Dänemark
- Mondex, in Swinton, England
- darüberhinaus wird unter CIN TC224 WG10 eine "intersect electronic purse" (branchenübergreifende elektronische Geldbörse) standardisiert.

In diesen bekannten Systemen wird grundsätzlich folgendes Verfahren verwendet:
Der erste Schritt ist das Laden von geldwerten Einheiten in die Chipkarte, wobei der Gegenwert, den der Karteninhaber in bar oder auch bargeldlos bezahlen muß, auf einem sogenannten "Pool-Konto" – des Börsenbetreibers hinterlegt wird. Bezahlt ein Karteninhaber anschließend mit seiner Chipkarte, werden geldwerte Einheiten aus der elektronischen Geldbörse herausgebucht und mit Hilfe eines Sicherheitsmoduls zum Terminal des Serviceanbieters übertragen. Dort werden die eingenommenen geldwerten Einheiten entweder zu einem Betrag akkumuliert und mit dem Börsenbetreiber abgerechnet oder aber jeder einzelne Bezahlvorgang wird beim Börsenbetreiber zur Abrechnung eingereicht. Akkumulierte Beträge oder einzelne Datensätze werden entweder auf einer sogenannten Händlerkarte gesammelt, die der Serviceanbieter einreichen muß oder mit einem entsprechenden ausgerüsteten Terminal online an eine Abrechnungsstelle übertragen.

Weiterhin sind elektronische Geldbörsenanwendungen bekannt, die auf einer Mikroprozessorkarte realisiert sind. Bei Mikroprozessoranwendungen erfolgt die Steuerung der Anwendung durch ein Chipkartenbetriebssystem, wie es beispielsweise im Standard prEN726-3 definiert ist. Auch diese Anwendung zeichnet sich dadurch aus, daß auf der Karte Geldbeträge gespeichert werden, die bei jeder Abbuchung um einen festgelegten Betrag reduziert werden. Der Vorteil der bekannten Mikroprozessorkarten gegenüber den bekannten Speicherkarten besteht darin, daß die Mikroprozessorkarten prüfen können, ob das abbuchende System authentisch ist oder umgekehrt. Diese Überprüfung ist bei einer Speicherchipkarte nicht möglich. Außerdem sind ähnliche Systeme und Verfahren durch die US-A-4,859,837, WO-A-90 15 382 und die DE 42 43 851 A1 realisiert. Außerdem ist noch ein Verfahren zur Transaktionskontrolle elektronischer Geldbörsensysteme in der DE 196 04 876 C1 beschrieben.

Die größte Verbreitung haben die Telefonkarten. Telefonkarten sind Speicherchipkarten mit einem Identifikationsbereich und mindestens einem Zählerbereich.

Außerdem ist unter der Bezeichnung Virtual Calling Card (VCC) in den USA ein Dienst eingeführt worden, der es dem Kunden ermöglicht, durch Angabe einer Zugangskennung in Verbindung mit einer PIN (Personal Identification Number), von jedem beliebigen Telefon aus zu telefonieren. Diese sogenannten Calling Card-Systeme basieren in der Regel auf einer zentralen Steuereinheit mit entsprechender Datenbank bzw. einem Zentralrechner. Die Gebührenabrechnung erfolgt dabei über ein dem Kunden zugeordnetes Konto. Dieser Dienst gewinnt zunehmend auch in Europa an Bedeutung. So ist zum Beispiel in "Deutsche Telekom AG – Vision", Februar 1995, Seiten 44 und 45, die T-Card mit Connect Service der Deutschen Telekom beschrieben.

In diesem Artikel ist auch ausgeführt, daß sich das Leistungsspektrum von der Telefonkarte bis hin zur Kreditkarte erstreckt. Zum Beispiel ist im Absatz 4.1.2.1., ab Seite 61 des Buches "Chipkarten als Werkzeug" von Beutelsberger, Kersten und Pfau beschrieben, wie Speicherchipkarten auf Authentizität durch Anwendung bekannter Challenge-Response Verfahren geprüft werden. Hit diesen Chipkarten ist es mit Hilfe eines Terminals bzw. eines Kartenlesers möglich, die Karten zu identifizieren und auf Plausibilität zu prüfen. In einem im Terminal eingebauten Sicherheitsmodul wird eine Authentifikation vorgenommen.

Weiterhin ist ein Verfahren zum Prüfen von Speicherchipkarten durch die DE 196 04 349 A1 bekannt, das eine zwei- oder mehrfache Authentifikation mit Hilfe kryptographischer Funktionen und mit Hilfe eines Terminals ermöglicht.

Der Nachteil der heute überwiegend benutzten Verfahren und Systeme besteht darin, daß der jeweilige Wert bzw. die Werteinheiten auf dem Datenträger, zum Beispiel der Chipkarte oder der Mikroprozessorkarte gespeichert ist/sind. Die Endgeräte erkennen den auf dem Datenträger gespeicherten Wert und erniedrigen entsprechend des Preises einer gekauften bzw. verkauften Dienstleistung den Wert auf dem Datenträger. Aufgrund der großen Anzahl von vorausbezahlten Datenträgern, die in Umlauf gebracht werden, wird in der Regel auf das Führen eines sogenannten Schattenkontos bzw. Schattensaldos in den Endgeräten und/oder deren Hintergrundsystemen verzichtet. Damit ist den Endgeräten und deren Hintergrundsystemen die Verifizierung, zum Beispiel des Sollwertes, eines sich in Gebrauch befindlichen Datenträgers nicht möglich. Durch Manipulation oder Fälschung des Datenträgers können somit Geld- oder Werteeinheiten erzeugt werden, die eigentlich dem Betreiber eines Buchungssystems zustünden. Die hierdurch für die Betreiber entstehenden Schäden werden derzeit weltweit monatlich auf einen zweistelligen Millionenbetrag geschätzt.

Die Systeme mit Schattenkonten bzw. Schattensalden haben den entscheidenden Nachteil, daß große Datenmengen im System übertragen werden müssen. Weiterhin sind viele Endgeräte nicht online angeschlossen, sondern übertragen erst mit einer Zeitverzögerung die Datensätze. Manipulationen sind somit nicht sofort erkennbar.

Der Erfindung liegt deshalb die Aufgabe zugrunde, ein Verfahren zur sicheren Handhabung von Geld- oder Werteeinheiten mit vorausbezahlten Datenträgern, wie zum Beispiel Chipkarten, Magnetstreifenkarten oder ähnliches, in elektronischen Buchungssystemen wie Telefonkartensystemen, Geldbörsensystemen und ähnliches zu schaffen, das eine Kartenmanipulation wertlos macht und das den gegebenenfalls hohen Datenübertragungsaufwand bei den bekannten Systemen reduziert.

Die erfindungsgemäße Lösung der Aufgabe ist im Kennzeichen des Patentanspruchs 1 charakterisiert.

Weitere Lösungen sind in dem jeweils kennzeichnenden Teil der Patentansprüche 2 bis 7 angegeben.

Durch das erfindungsgemäße Verfahren ist ein potentieller Betrüger bzw. Angreifer gezwungen, das Hintergrundsystem des Betreibers zu manipulieren oder zu scannen, das

heißt durchprobieren verschiedener Erkennungsmuster, um an den Gegenwert eines jeweiligen Datenträgers bzw. einer Chipkarte zu gelangen. Dies ist für den Betrüger wesentlich schwieriger in der Durchführung als die Manipulation des jeweiligen Datenträgers in Form einer Speicherchipkarte oder einer Mikroprozessorchipkarte. Für den Betreiber hingegen ist ein zentrales Hintergrundsystem in gesicherter Umgebung wesentlich einfacher gegen unerlaubte Zugriffe zu schützen. Findet zum Beispiel ein Betrüger durch Scannen ein Erkennungsmuster heraus, so steht ihm lediglich der Gegenwert dieses einen Datenträgers bzw. Erkennungsmusters zur Verfügung. Das Scannen des nächsten Erkennungsmusters erfordert von ihm wieder den gleichen hohen Aufwand. Wichtig ist, daß die Manipulation der Datenträger selbst durch dieses Verfahren zwecklos wird. Der Wert einer Kopie bzw. einer Simulation von Datenträgern würde sich auch nur auf den jeweiligen geringen aktuellen Wert des einzelnen Datenträgers beschränken. Außerdem hat das vorliegende Verfahren noch den Vorteil, daß es den hohen Datenübertragungsaufwand der bisher bekannten Verfahren mit Schattenkonten reduziert. Die Reaktionszeiten auf erkannte Sicherheitsprobleme im Hintergrundsystem werden im Vergleich zu dem bisherigen Verfahren wesentlich kürzer und die Zuordnung von Leistungsmerkmalen zur Identifikation kann jetzt im zentralen Rechner oder in der zentralen Steuereinheit des Hintergrundsystems vorgenommen werden.

Weitere Vorteile, Merkmale und Anwendungsmöglichkeiten der vorliegenden Erfindung, sowohl für den Netzbetreiber und den Diensteanbieter als auch für den Benutzer des Datenträgers ergeben sich aus der nachfolgenden Beschreibung in Verbindung mit dem in der Zeichnung dargestellten Ausführungsbeispielen.

Die Erfindung wird im folgenden anhand von in der Zeichnung dargestellten Ausführungsbeispielen näher beschrieben. In der Beschreibung, in den Patentansprüchen, der Zusammenfassung und in der Zeichnung werden die in der hinten angeführten Liste der Bezugszeichen verwendeten Begriffe und zugeordneten Bezugszeichen verwendet.

In der Zeichnung bedeutet:

Fig. 1 ein prinzipielles Operationsdiagramm des erfindungsgemäßen Verfahrens.

Bevor die detaillierte Funktionsweise und Wirkungsweise des erfindungsgemäßen Verfahrens anhand **Fig.** 1 erklärt wird, soll zunächst eine Beschreibung der grundsätzlichen Wirkungsweise und Verfahrensschritte folgen.

Ein Kunde erwirbt eine Telefonkarte. Die Telefonkarte enthält zum Beispiel in einem Chip gespeichert lediglich die Telefonkarten ID 12345. . . . Führt der Kunde die Karte in ein Kartentelefon ein, so liest dieses Telefon die ID aus und stellt eine Verbindung zum Hintergrundsystem her. Über diese Verbindung wird dem Hintergrundsystem die ID übermittelt. Das Hintergrundsystem kann daraufhin der ID einen Wert in Form von Einheiten oder DM zuordnen. Der Kunde beginnt nun mit der Wahl einer Telefonnummer. Die Wahlinformationen werden jedoch nicht vom Kartentelefon ausgewertet, sondern lediglich von dort an das Hintergrundsystem weitergeleitet. Hier werden die Wahlinformationen ausgewertet, die Verbindung wird entsprechend des noch vorhandenen Guthabens aufgebaut und bei erreichen des Guthabenwertes Null wieder getrennt.

Durch die Steuerung der Verbindung mittels eines zentralen Hintergrundsystems (ähnlich dem eines Calling Card-Systems) können fast alle erdenklichen Leistungen angeboten und einfach (da zentral) administriert und weiterentwickelt werden.

Weiterhin kann der ID zum Beispiel ein bestimmtes Tarifmodell zugeordnet werden (wurde die Karte = ID zum Beispiel im Rahmen einer Sonderaktion verkauft, mit der besonders günstige Verbindungskonditionen verknüpft waren, so kann dies durch Zuordnung eines entsprechenden Tarifmodells umgesetzt werden). Auf diese Art ist die Verknüpfung verschiedenster Leistungsmerkmale und Dienstleistungen möglich.

Durch das hier angegebene Verfahren ist es möglich, daß der außer Reichweite des jeweiligen Betreibers befindliche Datenträger des Nutzers bzw. Kunden, der sich hierdurch in einer unsicheren Umgebung befindet, nicht mehr den Geld- oder Einheitenwert enthält, sondern nur noch ein eindeutiges Erkennungsmuster, zum Beispiel eine Seriennummer, ein Kryptogramm, einen Kryptoschlüssel oder Äquivalentes. Das Erkennungsmuster wird vom Endgerät bei einem Nutzungsvorgang abgefragt. Der Datenträger identifiziert sich anhand des Erkennungsmusters einem Endgerät und seinem Hintergrundsystem bzw. Hintergrundsystemen gegenüber eindeutig. Der dem Datenträger zugeordnete Geld- oder Einheitenwert wird entsprechend einer verkauften oder gekauften Dienstleistung in den Hintergrundsystemen der Betreiber erniedrigt.

Um einem Angreifer bzw. potentiellen Betrüger den Zugang zu einem Erkennungsmuster, zum Beispiel durch Scannen, zu erschweren, ist das Erkennungsmuster möglichst komplex zu wählen und es kann überdies auch auf dem Datenträger kryptographisch gesichert abgelegt werden.

Das Erkennungsmuster ist als sogenannter öffentlicher kryptographischer Schlüssel ausgeführt, der für jeden Datenträger jeweils nur einmal existiert. Ein Endgerät/Hintergrundsystem sendet dem Datenträger eine sogenannte Challenge, die durch den Datenträger selbst mittels des auf dem Datenträger hinterlegten kryptographischen Schlüssel verschlüsselt wird. Das Ergebnis ist die sogenannte Antwort (Response). Sie wird dem Hintergrundsystem bzw. Endgerät des Betreibers zurückgesendet. Der in den Hintergrundsystemen des Betreibers hinterlegte sogenannte geheime Schlüssel zu genau diesem einen Datenträger wird vom Hintergrundsystem zur Entschlüsselung der Response verwendet. Stimmen Challenge und Response überein, dann ist der Datenträger authentisch. Außerdem ist eine zusätzliche Führung der Geld- und Werteeinheiten, gegebenenfalls kryptographisch gesichert, auf dem Datenträger zur Durchführung einer Plausibilitätskontrolle möglich.

In dem in **Fig.** 1 dargestellten prinzipiellen Verfahrensdiagramm finden die in der öffentlichen Telekommunikation üblichen Chipkarten in Form von Speicherchipkarten bzw. Mikroprozessorchipkarten Anwendung. Besondere Sicherheitseigenschaften dieser Chipkarten sind nicht erforderlich. Es ist lediglich bei der Personalisierung der Chipkarten zu beachten, daß das Identifikationsmerkmal zufällig aus einem um mehrere Dimensionen größeren Wertebereich gewählt wird. Beispiel: Herausgegebene Karten insgesamt = 10^6 Stück, Wertebereich = 10^{12}, woraus sich die Länge der Kartennummer zu 12 Stellen ergibt. Das Diagramm nach **Fig.** 1 ist grundsätzlich in die Telekommunikationsinfrastruktur I, den Kundenbereich II und in die Kommunikationswege III unterteilt.

Das Verfahren läuft nun wie folgt ab: Ein Speicher- bzw. Mikroprozessorchip einer zum Beispiel Telefonkarte wird durch den Kartenausgeber I A personalisiert, das heißt mit einem eindeutigen Identifikationsmerkmal, zum Beispiel einer Kartennummer, versehen. Diesem Identifikationsmerkmal wird ein Wert (zum Beispiel × DM oder × Einheiten) zugeordnet, der jedoch nicht im Chip gespeichert bzw. hinterlegt wird. Der Wert wird zusammen mit dem Identifikationsmerkmal dem Hintergrundsystem I B über den Kommunikationsweg III B verfügbar gemacht. Dort wird das Identifikationsmerkmal zusammen mit dem Wert in einer Daten-

bank gespeichert. Dabei erfolgt die Speicherung zunächst mit dem Vermerk "nicht freigeschaltet".

Unmittelbar vor dem Verkauf der Telefonkarte durch den Kartenausgeber wird der Vermerk "nicht freigeschaltet" in der Datenbank des Hintergrundsystems I B entfernt. Der Wert der jeweiligen Karte steht damit im Hintergrundsystem I B zur Abbuchung bereit. Nutzt nun ein Kunde II eine derartige Chipkarte II A an einem hierfür vorgesehenen öffentlichen Kommunikationsterminal I C, dann liest das Telekommunikationsterminal lediglich das Identifikationsmerkmal aus der Karte aus, um es an das Hintergrundsystem I B weiterzuleiten, das heißt es führt eine Prüfungsanfrage III D aus. Das Hintergrundsystem fügt nun dem Identifikationsmerkmal seinen ursprünglich bei der Personalisierung zugeordneten Wert zu und bei ausreichenden Guthaben wird die Kommunikation freigegeben, das heißt es folgt eine Buchungsbestätigung III E. Die Kommunikationsverbindung wird hierbei unmittelbar durch das Hintergrundsystem I B vermittelt und kontrolliert. Damit kann eine Verbindung nach Abbuchung des vollständigen Kartenwertes in der Datenbank des Hintergrundsystems I B durch dasselbe getrennt werden.

Liste der Bezugszeichen

I Telekommunikationsinfrastruktur
A Kartenherausgeber (Chipkartenpersonalisierung)
B Hintergrundsystem (mit Datenbank)
C Kommunikationsterminal oder Endgerät
II Kunde
A Chipkarte oder Datenträger
III Kommunikationswege
A Chipkartenausgabe
B Übermittlung Personalisierungsdaten
C Chipkartennutzung
D Buchungsanfrage
E Buchungsbestätigung

Patentansprüche

1. Verfahren zur sicheren Behandlung bzw. Handhabung von Geld- oder Werteinheiten mit vorausbezahlten Datenträgern, wie zum Beispiel Chipkarten oder Magnetstreifenkarten in elektronischen Buchungssystemen für zum Beispiel Telefonkartensysteme, Geldbörsensysteme oder äquivalente Systeme, **dadurch gekennzeichnet,**
daß der von einem Kunden oder Nutzer vorausbezahlte Datenträger (II A) nur noch ein eindeutiges Erkennungsmuster bzw. Identifikationsmerkmal, wie zum Beispiel eine Seriennummer, ein Kryptogramm, einen Kryptoschlüssel oder ähnliches aufweist, und vom Kartenausgeber (I A) personalisiert wird,
daß dem Erkennungsmuster bzw. Identifikationsmerkmal ein Wert zugeordnet wird, die beide zusammen einem Hintergrundsystem (I B) über einen Kommunikationsweg (III B) zur Übermittlung der Personalisierungsdaten verfügbar gemacht werden, dort gespeichert und zunächst mit einem Vermerk "nicht freigeschaltet" versehen werden,
daß unmittelbar vor oder beim Verkauf des zugehörigen Datenträgers der Vermerk in der Datenbank des Hintergrundsystems (I B) entfernt wird,
daß dieses Erkennungsmuster einem Endgerät (II C) und/oder seinem(n) Hintergrundsystem bzw. -systemen bei einem Nutzungsvorgang automatisch ohne Zutun des Nutzers zugeführt wird, indem es abgefragt wird, wobei die Eingabe weiterer Identifikationsmerkmale durch den Nutzer optional möglich ist,
daß der Datenträger (II A) anhand des Erkennungsmusters sich eindeutig dem Endgerät und/oder seinem/seinen Hintergrundsystem(en) (I B) gegenüber identifiziert und
daß dann darauffolgend der dem Datenträger (II A) zugeordnete Geld- oder Einheitenwert entsprechend einer verkauften bzw. gekauften Dienstleistung im Hintergrundsystem (I B) des Betreibers automatisch verringert und verwaltet wird.

2. Verfahren nach Patentanspruch 1, dadurch gekennzeichnet,
daß das Hintergrundsystem (I B) die Kommunikationsverbindung unmittelbar vermittelt und kontrolliert,
daß das Erkennungsmuster des Datenträgers (II A) ein sogenannter öffentlicher kryptographischer Schlüssel ist, der für jeden Datenträger jeweils nur einmal existiert und
daß dem Schlüssel bzw. einer I D ein bestimmtes Tarifmodell zugeordnet wird.

3. Verfahren nach Patentanspruch 2, dadurch gekennzeichnet, daß das jeweilige Buchungssystem den zugehörigen geheimen Schlüssel kennt und den Datenträger anhand eines Challenge/Response-Verfahrens authentifiziert.

4. Verfahren nach einem der Patentansprüche 1 bis 3, dadurch gekennzeichnet, daß die Kommunikation zwischen den Endgeräten und dem Hintergrundsystem bzw. den Hintergrundsystemen der jeweiligen Netzknoten erfolgt.

5. Verfahren nach einem der Patentansprüche 1 bis 4, dadurch gekennzeichnet, daß eine zusätzliche Führung der Geld- oder Werteeinheiten, gegebenenfalls kryptographisch gesichert, auf dem jeweiligen Datenträger zur Durchführung einer Plausibilitätskontrolle erfolgt.

6. Verfahren nach einem der Patentansprüche 1 bis 5, dadurch gekennzeichnet,
daß der in dem/den Hintergrundsystem(en) des Betreibers hinterlegte geheime Schlüssel zu nur einem bestimmten Datenträger vom Hintergrundsystem zur Entschlüsselung der Antwort (Response) verwendet wird und
daß bei Übereinstimmung von Challenge und Response der Datenträger als authentisch klassifiziert wird.

7. Verfahren nach einem der Patentansprüche 1 bis 6, dadurch gekennzeichnet, daß zum Erschweren des Scannens durch eine unbefugte Person das Erkennungsmuster komplex ausgeführt wird.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

BNSDOCID: <DE 19860203A1 I >

Nummer: DE 198 60 203 A1
Int. Cl.[7]: G 06 F 17/60
Offenlegungstag: 29. Juni 2000

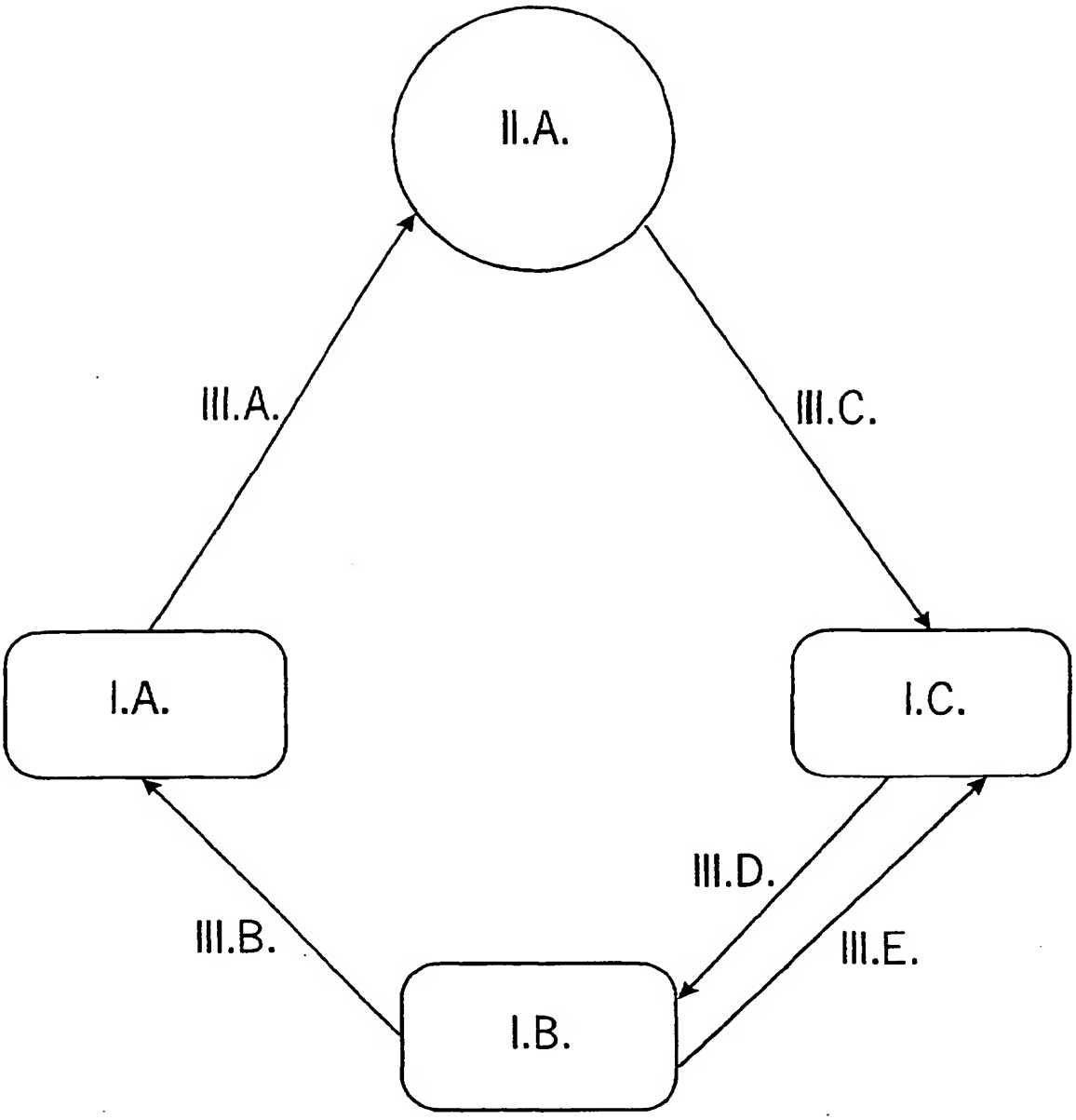


FIG. 1